



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Handwritten signature

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/966,227	09/27/2001	Jeffrey Scott Bardsley	RSW920010166US1	5924
30449 7590 02/26/2007 SCHMEISER, OLSEN & WATTS 22 CENTURY HILL DRIVE SUITE 302 LATHAM, NY 12110			EXAMINER HENNING, MATTHEW T	
			ART UNIT 2131	PAPER NUMBER
SHORTENED STATUTORY PERIOD OF RESPONSE 3 MONTHS			MAIL DATE 02/26/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary

Application No.

09/966,227

Applicant(s)

BARDSLEY ET AL.

Examiner

Matthew T. Henning

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 08 December 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 5-7, 10-12 and 19-32 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 5-7, 10-12 and 19-32 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 27 November 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- ☐ Notice of Informal Patent Application
- ☐ Other: _____

Art Unit: 2131

1 This action is in response to the communication filed on 12/08/2006.

2 **DETAILED ACTION**

3 ***Continued Examination Under 37 CFR 1.114***

4 A request for continued examination under 37 CFR 1.114, including the fee set forth in
5 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is
6 eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e)
7 has been timely paid, the finality of the previous Office action has been withdrawn pursuant to
8 37 CFR 1.114. Applicant's submission filed on 11/08/2006 has been entered.

9
10 ***Response to Arguments***

11 Applicant's arguments filed 11/08/2006 have been fully considered but they are not
12 persuasive.

13 Regarding applicants' argument that Sharma does not teach performing the determining
14 and comparing steps **for each occurrence of the value of the signature event counter**
15 **exceeding the threshold quantity**, the examiner does not find the argument persuasive. The
16 examiner notes that the applicants appear to be using the terminology "each occurrence"
17 incorrectly in that the applicants appear to be arguing that this limitation requires that the steps
18 are performed for all occurrences over all time. However, "each occurrence" actually requires
19 only the occurrences over a group of two or more. As such, Sharma teaches that for each
20 occurrence after the first 1000 occurrences of generating an alert, the determining and comparing
21 is performed, as required by the claim language. As such, it can be seen that the teachings of
22 Sharma teach the claimed invention, in addition to the 1000 initial alerts. The combination of

Art Unit: 2131

Vaidya and Sharma, when viewed at any point in time after the first 1000 alerts, meets the claim limitations, in that "for each occurrence...". Therefore, the examiner does not find the argument persuasive.

Regarding applicants' arguments that because Vaidya does not refer to its log as a "log" but rather as a state cache, that Vaidya does not teach purging expired entries from a log before determining the rate, the examiner does not find the argument persuasive. Vaidya clearly teaches that when determining a rate, which is the number of occurrences over a period of time, that stale entries (older than a predetermined time) in the state cache (log) should be purged. As such, the examiner does not find the argument persuasive.

Claims 5-7, 10-12, and 19-32 have been examined, while claims 1-4, 8-9, and 13-18 have been cancelled.

All objections and rejections not set forth below have been withdrawn.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 5, 10, and 19-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vaidya (US Patent Number 6,279,113), and further in view of Sharma et al. (US Patent Number 6,909,692) hereinafter referred to as Sharma

Art Unit: 2131

1 Regarding claim 5, Vaidya disclosed a method of operating an intrusion detection system,
2 comprising the steps of: monitoring, by the intrusion detection system, for occurrence of a
3 signature event that is indicative of a DOS intrusion on a protected device, said DOS attack
4 attempting to impede operation of the protected device (See Vaidya Abstract and Col. 12
5 Paragraphs 2-3); when a signature event occurs, increasing a value of a signature event counter
6 and comparing the value of the signature event counter with a signature threshold quantity (See
7 Vaidya Col. 12 Lines 26-36); for each occurrence of the value of the signature event counter
8 exceeding the signature threshold quantity, generating an alert by the intrusion detection sensor
9 of the intrusion detection system (See Vaidya Col. 12 Lines 36-41, Col. 11 Lines 5-8, and Col. 6
10 Lines 20-26); but Vaidya failed to disclose recording a time for generating the alert in a log of a
11 governor comprised by the intrusion detection sensor, determining from the contents of the log a
12 present alert generation rate, and comparing the present alert generation rate with an alert
13 generation rate threshold, wherein said recording is performed after said generating is performed,
14 wherein said determining is performed after said recording is performed, and wherein said
15 comparing the present alert generation rate with the alert generation rate threshold is performed
16 after said determining is performed; or when the present alert generation rate exceeds the alert
17 generation rate threshold, altering an element of a signature set of the intrusion detection system
18 to decrease an alert generation rate of the intrusion detection system.

19 Sharma teaches that generating too many alerts in a network management system can
20 crash the system (See Sharma Col. 3 Paragraph 3) and further teaches that in order to control the
21 alert generation rate, each alert should be logged including a time of the alert (See Sharma Col. 8
22 Line 61 – Col. 9 Line 15), an alert generation rate should be determined using the log (See

Art Unit: 2131

1 Sharma Col. 9 Lines 16-25), the determined rate should be compared with a threshold (See
2 Sharma Col. 9 Lines 25-27), and when the rate is too high, altering the management system to
3 decrease an alert generation rate of the system (See Sharma Col. 9 Line 28 – Col. 10 Line 15 and
4 Col. 7 Lines 1-23).

5 It would have been obvious to the ordinary person skilled in the art at the time of
6 invention to employ the teachings of Sharma in the IDS system of Vaidya by the reaction module
7 logging the alerts, determining the alert generation rate, comparing the rate to the threshold rate,
8 and if greater than the threshold altering the attack signature profile to indicate a new threshold
9 for event rate in order to begin transmitting alerts again. This would have been obvious because
10 the ordinary person skilled in the art would have been motivated to protect the system
11 administrator from being over informed as well as protecting the management system from
12 crashing.

13 Regarding claim 10, Vaidya disclosed programmable media containing programmable
14 software for operation of an intrusion detection system, programmable software comprising the
15 steps of: monitoring, by the intrusion detection system, for occurrence of a signature event that is
16 indicative of a DOS intrusion on a protected device, said DOS attack attempting to impede
17 operation of the protected device (See Vaidya Abstract and Col. 12 Paragraphs 2-3); when a
18 signature event occurs, increasing a value of a signature event counter and comparing the value
19 of the signature event counter with a signature threshold quantity (See Vaidya Col. 12 Lines 26-
20 36); for each occurrence of the value of the signature event counter exceeding the signature
21 threshold quantity, generating an alert by the intrusion detection sensor of the intrusion detection
22 system (See Vaidya Col. 12 Lines 36-41, Col. 11 Lines 5-8, and Col. 6 Lines 20-26); but Vaidya

Art Unit: 2131

1 failed to disclose recording a time for generating the alert in a log of a governor comprised by the
2 intrusion detection sensor, determining from the contents of the log a present alert generation
3 rate, and comparing the present alert generation rate with an alert generation rate threshold,
4 wherein said determining is performed after said recording is performed, and wherein said
5 comparing the present alert generation rate with the alert generation rate threshold is performed
6 after said determining is performed;; or when the present alert generation rate exceeds the alert
7 generation rate threshold, altering an element of a signature set of the intrusion detection system
8 to decrease an alert generation rate of the intrusion detection system.

9 Sharma teaches that generating too many alerts in a network management system can
10 crash the system (See Sharma Col. 3 Paragraph 3) and further teaches that in order to control the
11 alert generation rate, each alert should be logged including a time of the alert (See Sharma Col. 8
12 Line 61 – Col. 9 Line 15), an alert generation rate should be determined using the log (See
13 Sharma Col. 9 Lines 16-25), the determined rate should be compared with a threshold (See
14 Sharma Col. 9 Lines 25-27), and when the rate is too high, altering the management system to
15 decrease an alert generation rate of the system (See Sharma Col. 9 Line 28 – Col. 10 Line 15 and
16 Col. 7 Lines 1-23).

17 It would have been obvious to the ordinary person skilled in the art at the time of
18 invention to employ the teachings of Sharma in the IDS system of Vaidya by the reaction module
19 logging the alerts, determining the alert generation rate, comparing the rate to the threshold rate,
20 and if greater than the threshold altering the attack signature profile to indicate a new threshold
21 for event rate in order to begin transmitting alerts again. This would have been obvious because
22 the ordinary person skilled in the art would have been motivated to protect the system

Art Unit: 2131

1 administrator from being over informed as well as protecting the management system from
2 crashing.

3 Regarding claims 19 and 25, Vaidya and Sharma disclosed alerting an administrator of
4 suspected DOS intrusions upon the protected device (See Vaidya Col. 6 Lines 20-26).

5 Regarding claims 20 and 26, Vaidya and Sharma disclosed that the alert generation rate
6 threshold is comprised by the governor (See Sharma Col. 9 Lines 16-26).

7 Regarding claims 21 and 27, Vaidya and Sharma disclosed that the signature set
8 comprises a unique signature set identifier (See Vaidya Col. 10 Lines 25-45 "Pattern"), the
9 signature event (See Vaidya Col. 10 Lines 25-45 "Attack_Signature"), the signature event
10 counter (See Vaidya Col. 12 Paragraph 3 "counter"), the signature threshold quantity (See
11 Vaidya Col. 12 Paragraph 3 "threshold"), and a signature threshold interval that specifies a
12 sliding time window (See Vaidya Col. 12 Paragraph 3 "predetermined time interval").

13 Regarding claims 22 and 28, Vaidya and Sharma disclosed that the protected device is
14 selected from the group consisting of a computer, a web server, and a workstation (See Vaidya
15 Col. 10 Lines 54-57).

16 Regarding claims 23 and 29, Vaidya and Sharma disclosed entering into the log a list of
17 timestamps that record the times at which the intrusion detection sensor generates alerts, wherein
18 said determining from contents of the log a present alert generation rate utilizes the timestamps
19 in the log (See Sharma Col. 9 Paragraph 2).

20 Regarding claims 24 and 30, Vaidya and Sharma disclosed that for each occurrence of
21 the value of the signature event counter exceeding the signature threshold quantity: after
22 generating the alert and before determining from contents of the log the present alert generation

Art Unit: 2131

1 rate, the method further comprises the step of: clearing the log of any entries that are past a
2 specific age (See Sharma Col. 9 Paragraph 2 and Vaidya Col. 12 Paragraph 2 wherein Vaidya
3 disclosed purging the expired entries of a log prior to determining the generation rate associated
4 with the log).

5 Claims 6, and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over the
6 combination of Vaidya and Sharma as applied to claims 5, and 10 above respectively, and further
7 in view of Lunt (Detecting Intruders in Computer Systems).

8 Vaidya and Sharma disclosed altering the signature set in order to reduce the frequency
9 of alert generation by halting the alert generation (See the rejection of claim 5 above), but failed
10 to disclose altering the threshold quantity in order to do so.

11 Lunt teaches that alarms do not always pertain to individual events, and because they can
12 come very quickly, after the first alarm is generated, subsequent alarms should be suppressed
13 until a second threshold, greater than the first, is reached (See Lunt Page 14 Lines 11-17).

14 It would have been obvious to the ordinary person skilled in the art at the time of
15 invention to employ the teachings of Lunt in the alert generation system of Vaidya and Sharma,
16 by suppressing alerts after the first threshold was reached, until a higher threshold is reached.
17 This would have been obvious because the ordinary person skilled in the art would have
18 recognized that multiple attacks can occur at the same time and would not want to ignore attacks
19 after the first initial attack.

20 Claims 7, and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over the
21 combination of Vaidya and Sharma as applied to claims 5, and 10 above respectively, and further
22 in view of Martin et al. (US Patent Number 6,772,349) hereinafter referred to as Martin.

Art Unit: 2131

1 Vaidya and Sharma disclosed altering the signature set in order to reduce the frequency
2 of alert generation by halting the alert generation (See the rejection of claim 5 above) and that
3 the generation rate was determined using a sliding time window (See Vaidya Col. 12 Paragraph
4 2), but failed to disclose altering the threshold interval in order to do so.

5 Martin teaches that in a network intrusion detection system, the time interval used to
6 collect signature data is indirectly proportional to the number of false alarms detected (See
7 Martin Col. 5 Lines 30-38).

8 It would have been obvious to the ordinary person skilled in the art at the time of
9 invention to employ the teachings of Martin in the alert suppressing system of Vaidya and
10 Sharma, by decreasing the time interval once the threshold was broken. This would have been
11 obvious because the ordinary person skilled in the art would have been motivated to ensure that
12 legitimate alerts were detected while false alarms were reduced.

13 Claims 31-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over the
14 combination of Vaidya and Sharma as applied to claims 5 and 10 above, and further in view of
15 Narendran et al. (US Patent Number 6,070,191) hereinafter referred to as Narendran.

16 The combination of Vaidya and Sharma taught clearing the log of any entries that are
17 past a specified permissible age (See teachings of Vaidya in Col. 12 Paragraph 2), determining
18 from contents of the log the current alert generation rate (See Sharma Col. 8 Line 61 – Col. 9
19 Line 27), and comparing the current alert generation rate with the alert generation rate threshold;
20 and for each occurrence of the current alert generation rate exceeding the alert generation rate
21 threshold (See Sharma Col. 8 Line 61 – Col. 9 Line 27); ascertaining that a signature set of the
22 intrusion detection system is at its initial state at which no changes in the signature set have been

Art Unit: 2131

1 made by the governor (See Sharma Col. 9 Line 54 – Col. 10 Line 15 wherein it would have been
2 inherent to determine which stage of the signature set was currently in use in order to ascertain
3 which step to perform), and altering one or more elements of the signature set in response to said
4 ascertaining (See Sharma Col. 9 Line 54 – Col. 10 Line 15), but failed to teach awaiting, by the
5 governor, for occurrence of a scheduled update time, and for each scheduled update time
6 occurrence, performing said steps.

7 Narendran teaches that in order to smooth out dynamic rate changes in a rate calculation
8 system, the rate should be calculated periodically over a “sliding window” (See Narendran Col.
9 16 Lines 25-32).

10 It would have been obvious to the ordinary person skilled in the art at the time of
11 invention to employ the teachings of Narendran in the system of Vaidya and Sharma by
12 periodically calculating the generation rate over a moving window. This would have been
13 obvious because the ordinary person skilled in the art would have been motivated to smooth out
14 dynamic rate changes in the rate determination system.

15 *Conclusion*


16 Claims 5-7, 10-12, and 19-32 have been rejected.

17 Any inquiry concerning this communication or earlier communications from the
18 examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790.
19 The examiner can normally be reached on M-F 8-4.

20 If attempts to reach the examiner by telephone are unsuccessful, the examiner's
21 supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the
22 organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2131

1 Information regarding the status of an application may be obtained from the Patent
2 Application Information Retrieval (PAIR) system. Status information for published applications
3 may be obtained from either Private PAIR or Public PAIR. Status information for unpublished
4 applications is available through Private PAIR only. For more information about the PAIR
5 system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR
6 system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

7
8
9
10
11
12 
13
14 Matthew Henning
15 Assistant Examiner
16 Art Unit 2131
17 2/22/2007


AYAZ SHEKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100